

Entra ID를 통한 보안 액세스를 위해 사용자 및 그룹 프로비저닝

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[Cisco Secure Access 구성](#)

[Microsoft Entra ID에서 프로비저닝 구성](#)

[다음을 확인합니다.](#)

[Cisco Secure Access의 Verity](#)

[Entra ID에서 확인](#)

[관련 정보](#)

소개

이 문서에서는 Entra ID에서 Cisco Secure Access로 사용자와 그룹을 프로비저닝하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- 주문 ID

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

- Cisco 보안 액세스 대시보드에 대한 관리자 액세스
- Entra ID 대시보드에 대한 관리자 액세스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Secure Access는 Microsoft Enterprise ID(이전의 Azure Active Directory)에서 사용자 및 그룹의 프로비저닝을 지원합니다.

이러한 프로비저닝을 통해 보안 액세스는 다음 권한을 부여받은 사용자 디렉토리를 유지 관리할 수 있습니다.

- ZTA(Zero Trust Access)에 등록
- VPNaaS에 연결합니다.
- Umbrella Roaming 사용자에게 ID 기반 정책을 적용합니다.



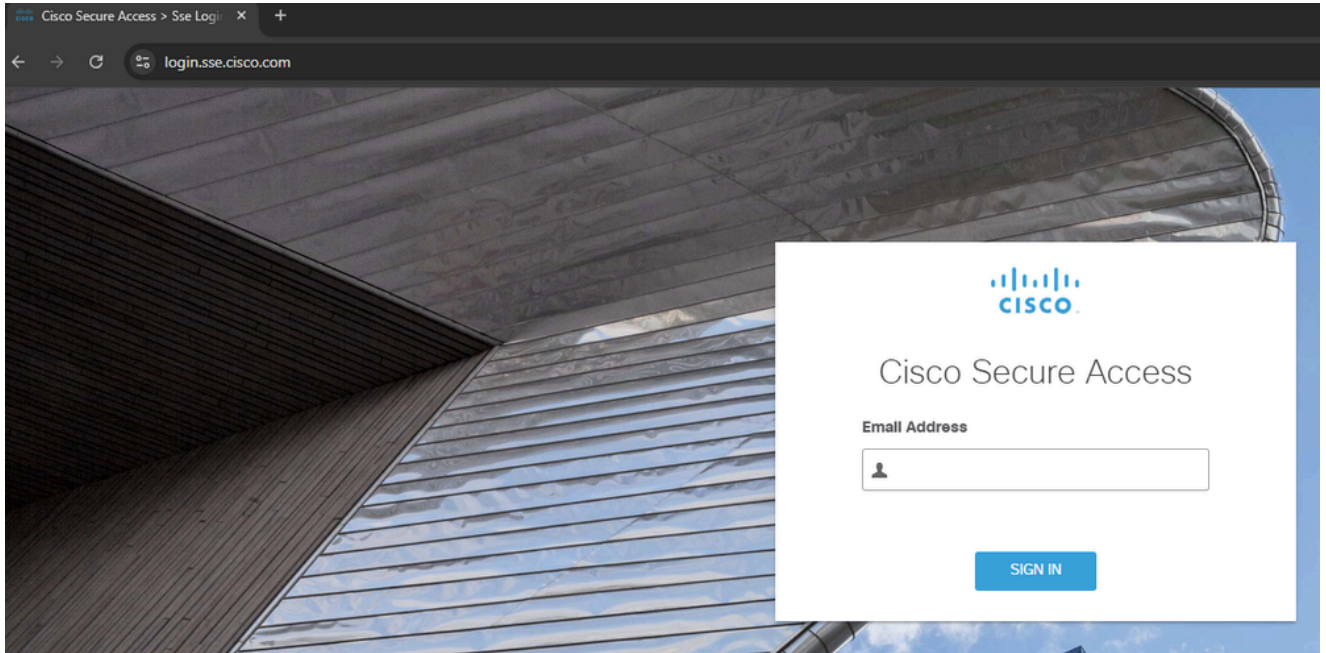
참고: 이 문서에서는 Entra ID의 사용자 및 그룹 프로비저닝에 특히 중점을 둡니다. ZTA 등록, VPNaaS 인증 또는 특정 Umbrella Roaming 설정을 위한 Entra ID 또는 기타 IdP(Identity Providers)의 컨피그레이션은 이 가이드의 범위를 벗어납니다.

구성

Cisco Secure Access 구성

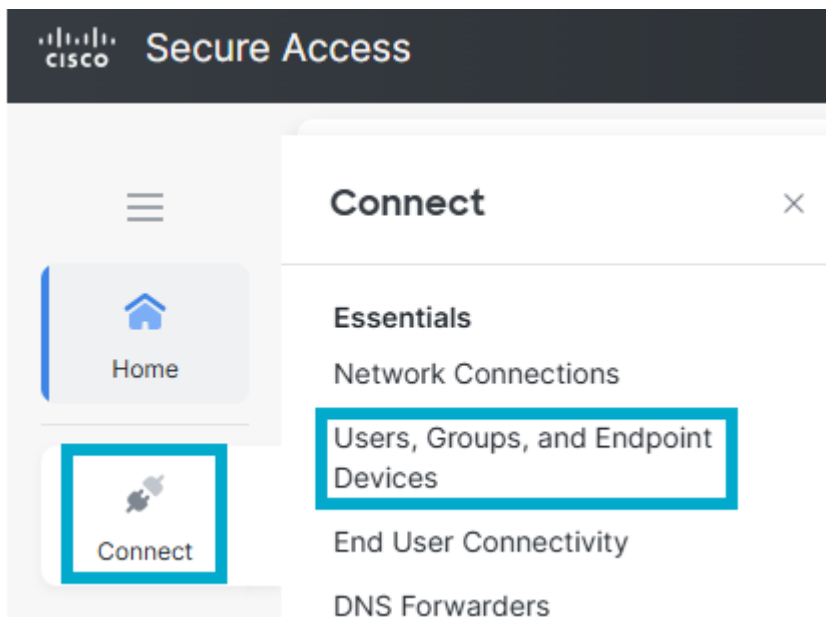
프로비저닝 프로세스를 시작하려면 먼저 Cisco Secure Access 대시보드 내에서 디렉토리 통합을 구성해야 합니다. 이 단계에서는 Microsoft Entra ID와의 보안 연결을 설정하는 데 필요한 자격 증명 및 구성 매개 변수를 생성합니다.

1. Cisco Secure Access Dashboard에 [로그인](#).



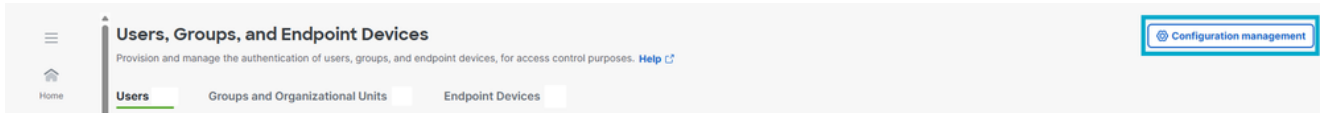
CSA에 로그인

2. Connect(연결) > Users, Groups and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스)로 이동합니다.



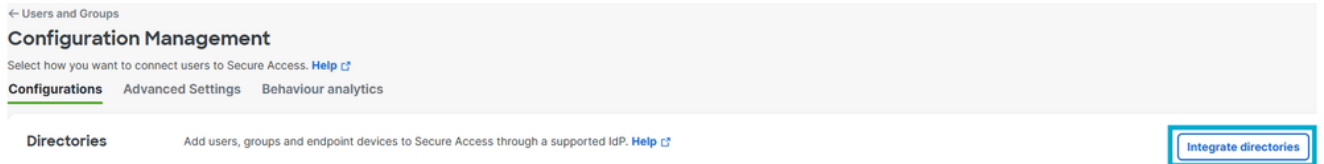
사용자 및 그룹

3. Configuration management(컨피그레이션 관리)를 클릭합니다.



컨피그레이션 관리

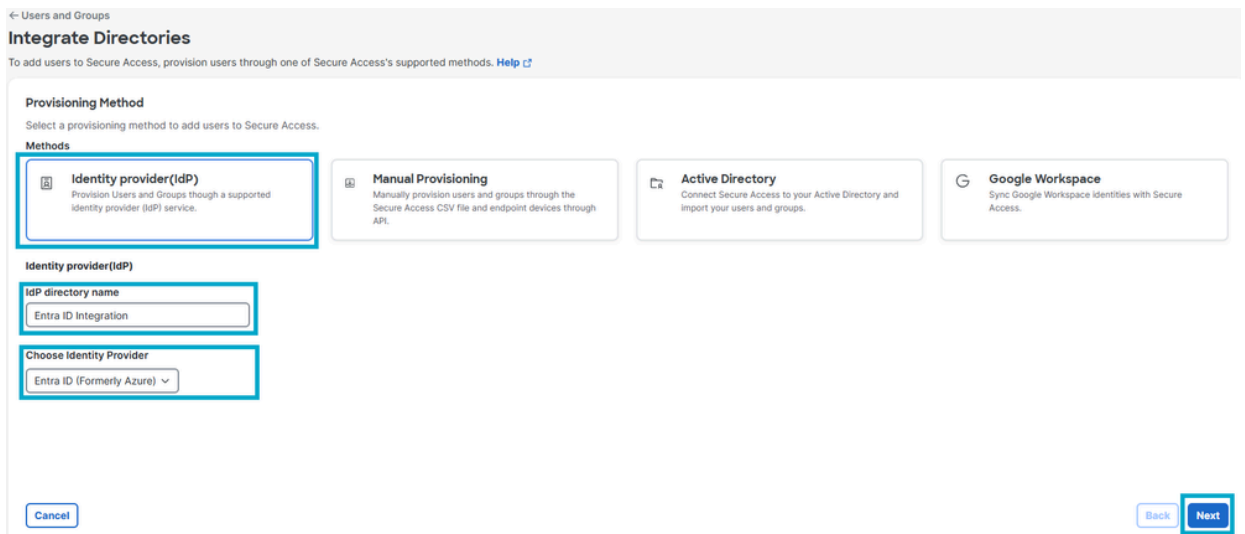
4. 디렉토리 통합을 클릭합니다.



Integrate Directory

5. Provision Method(프로비저닝 방법)에서 Identity Provider(ID 제공자)를 클릭합니다.

- IdP 디렉터리 이름: ID 통합.
- ID 공급자 선택: Entra ID(이전의 Azure)입니다.
- Next(다음)를 클릭합니다.



디렉토리 구성

6. 토큰 생성을 누릅니다. 생성된 토큰 및 프로비전 URL을 저장한 다음 완료를 누릅니다.

← Users and Groups

Entra ID Integration

Entra ID (Formerly Azure)

Follow the instructions below to provision identities to this directory. [Help](#)

Start Provisioning

To provision users to Secure Access, you must authenticate to your identity provider (IdP). Generate a token and then use it and the listed provisioning URL to provision users through your IdP. [Help](#)

Provisioning token

Once generated, copy and save this authentication token. It is required when configuring your IdP.

⚠ For security reasons, your token will only be displayed once. For future reference, copy this token and keep it in a safe place

Token:
[Copy token](#)

Generated On: March 17, 2026

Provisioning URL

Copy and save this provisioning URL. It is required when configuring your IdP.

[Copy URL](#)

Configure your IdP portal

Use the generated authentication token and provisioning URL to set up Secure Access in your IdP. Once setup, you can provision users to Secure Access. [Help](#)

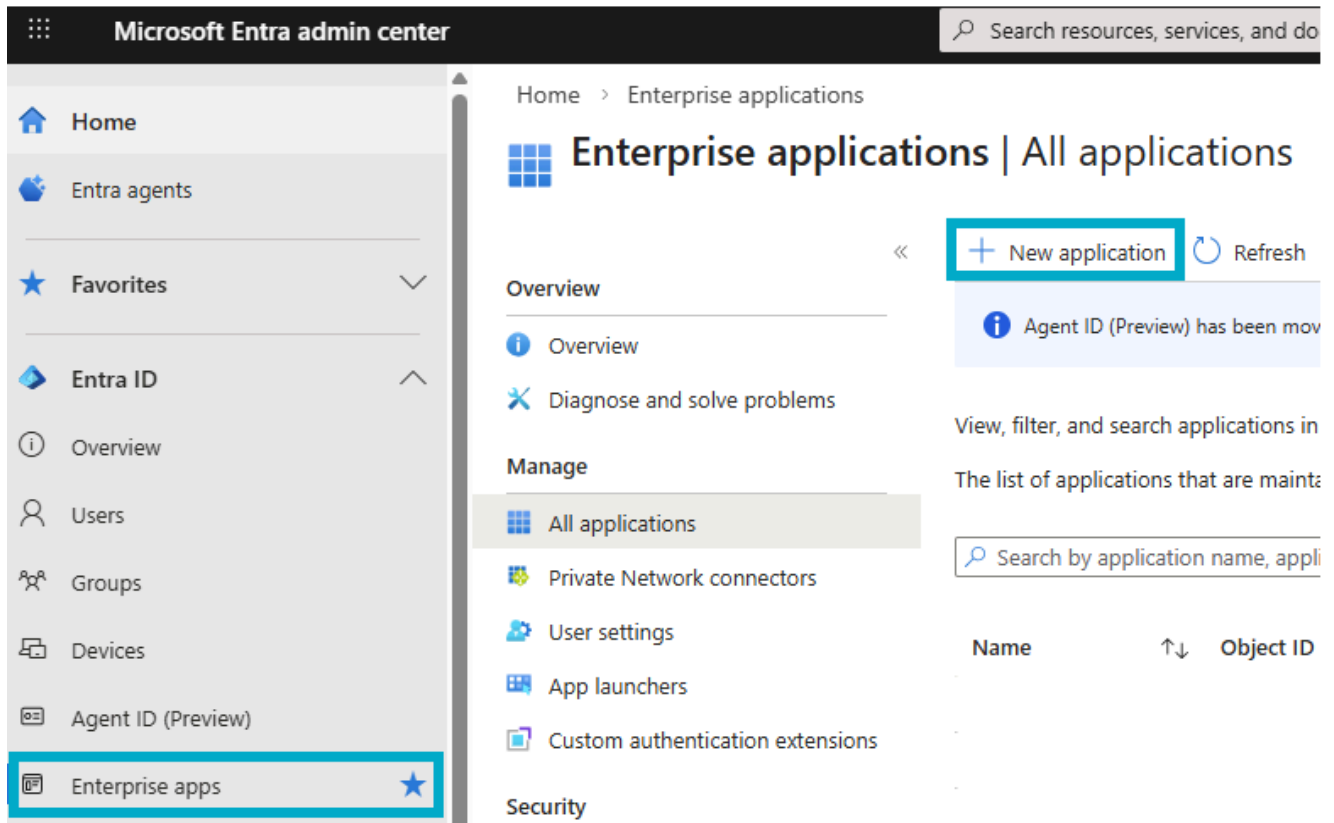
[Cancel](#) [Back](#) [Done](#)

토큰 생성

Microsoft Entra ID에서 프로비저닝 구성

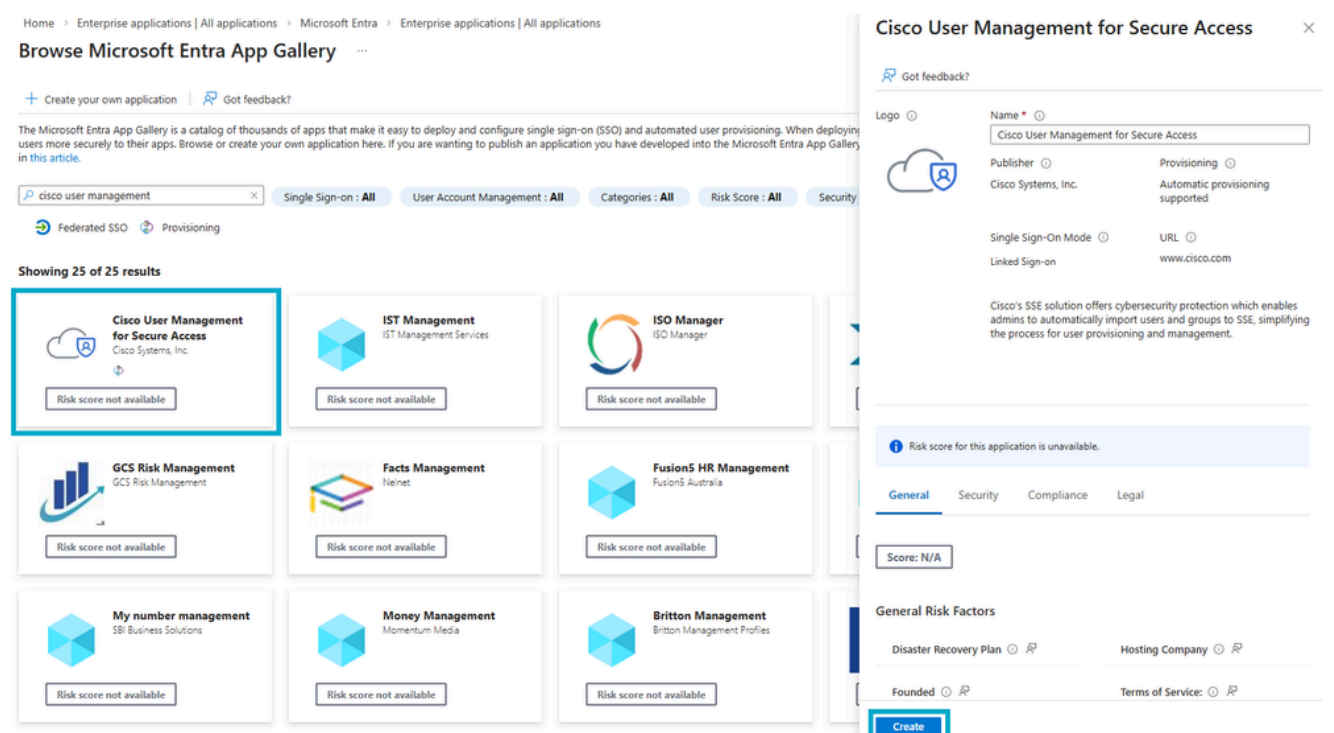
Cisco Secure Access 대시보드에서 자격 증명을 생성한 후에는 사용자 및 그룹의 동기화를 활성화 하도록 Microsoft Centera ID 테넌트 내에서 프로비저닝 설정을 구성해야 합니다.

1. Entra [ID에 로그인합니다.](#)
2. Enterprise Apps(엔터프라이즈 애플리케이션) > New Application(새 애플리케이션)으로 이동 합니다..



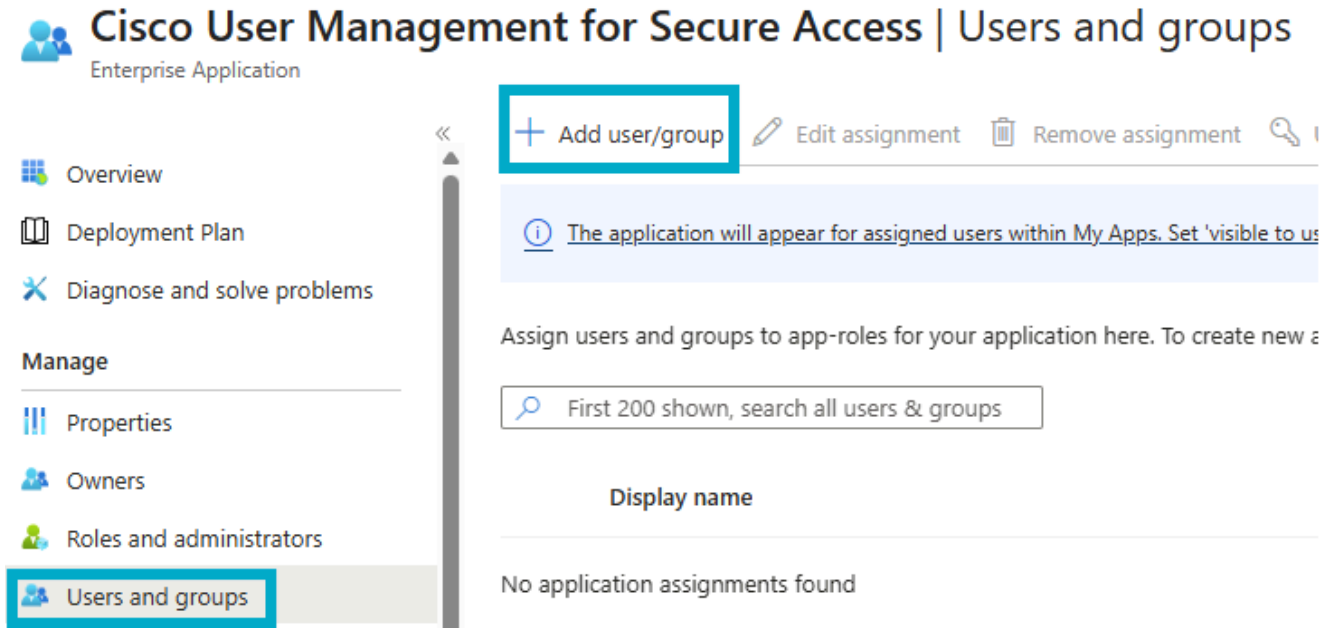
새 엔터프라이즈 앱

3. Entra App Gallery에서 Cisco User Management for Secure Access를 찾고 Create(생성)를 클릭합니다.



New App

4. Users and Groups(사용자 및 그룹) > Add user/group(사용자/그룹 추가)으로 이동합니다.



사용자 및 그룹 입력

5. Cisco Secure Access에 프로비저닝할 사용자/그룹을 지정하고 선택 및 할당을 클릭합니다.

Add Assignment

MSFT

⚠ When you assign a group to an application, only users directly in the group will have access. Access does not cascade to nested groups.

Users and groups

2 groups selected.

Select a role

User

Assign

Users and groups

🔍 Try changing or adding filters if you don't see what you're looking for

Search

IT

2 results found

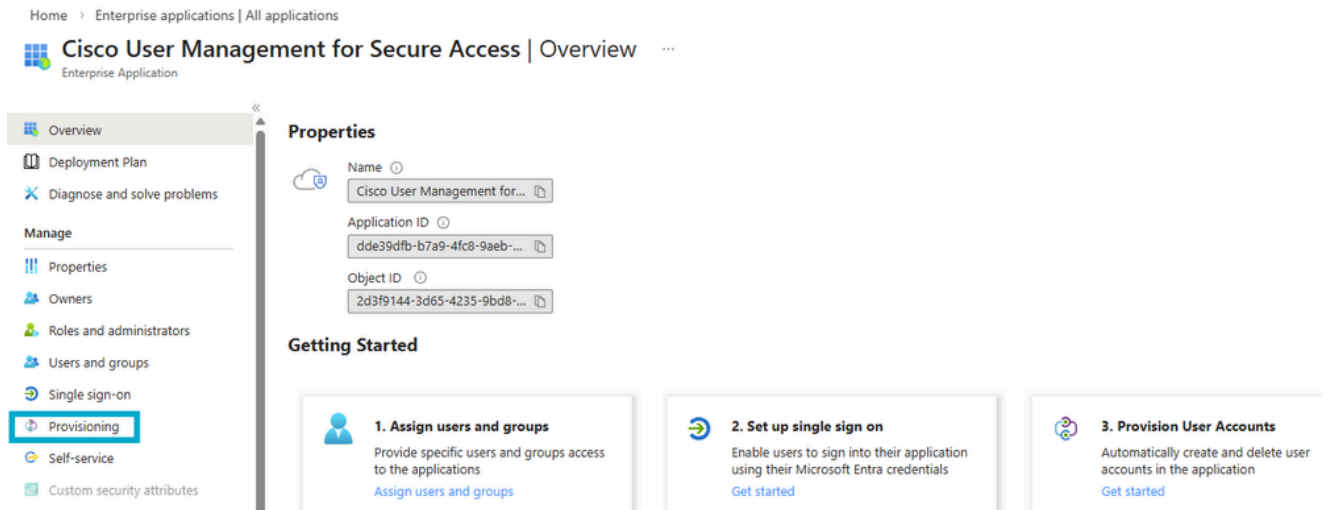
All Users Agent users Groups

	Name	Type
<input checked="" type="checkbox"/>	IT-Admins	Group
<input checked="" type="checkbox"/>	IT-Cloud-Admins	Group

Select

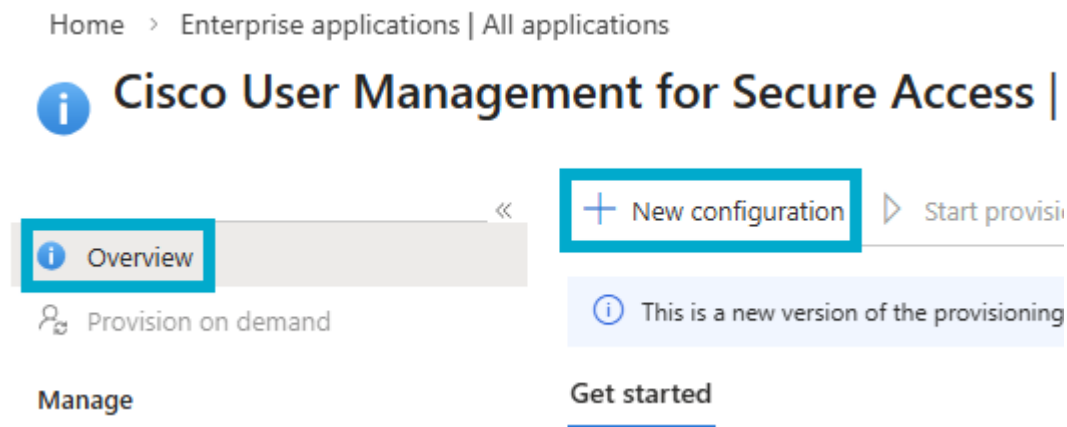
Assign Users and Groups

6. Provisioning(프로비저닝)으로 이동합니다.



Entra ID 프로비저닝

7. Overview(개요)를 클릭한 다음 New Configuration(새 컨피그레이션)을 클릭합니다.



새 컨피그레이션

8. 보안 액세스 컨피그레이션의 #6단계에서 저장된 테넌트 URL 및 비밀 토큰을 입력합니다. Test Configuration(컨피그레이션 테스트)을 클릭한 다음 Create(생성)를 클릭합니다. 컨피그레이션을 생성한 후에는 컨피그레이션 세부사항 페이지로 이동하여 고급 설정을 관리합니다.

New provisioning configuration

Microsoft Entra ID

Got feedback?

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user experience using the "Got feedback" button. [Click here to switch to the legacy experience.](#)

Create a provisioning configuration by completing the setup below. You can edit attribute mappings, scoping rules, and other settings later in the setup. [Learn more](#)

Admin credentials

Create automatic provisioning configuration for "Cisco User Management for Secure Access". A successful test connection may be required to proceed.

Tenant URL
Secret token

Test connection

Next steps:

After creating your configuration with default parameters, you will be taken to the configuration details page to manage advanced settings.

Create Cancel

Provisioning test connection
Connection test for "Cisco User Management for Secure Access" was successful.

테스트 통합

9. Overview(개요) > Start Provisioning(프로비저닝 시작)으로 이동합니다.

Home > Enterprise applications | All applications > Cisco User Management for Secure Access | Overview > New provisioning configuration

Cisco User Management for Secure Access | Overview

Overview Start provisioning Pause provisioning Restart provisioning Delete configuration Refresh Got feedback?

Provision on demand

Get started Overview Properties

Start provisioning
Start in progress

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user experience using the "Got feedback" button. [Click here to switch to the legacy experience.](#)

프로비저닝 시작

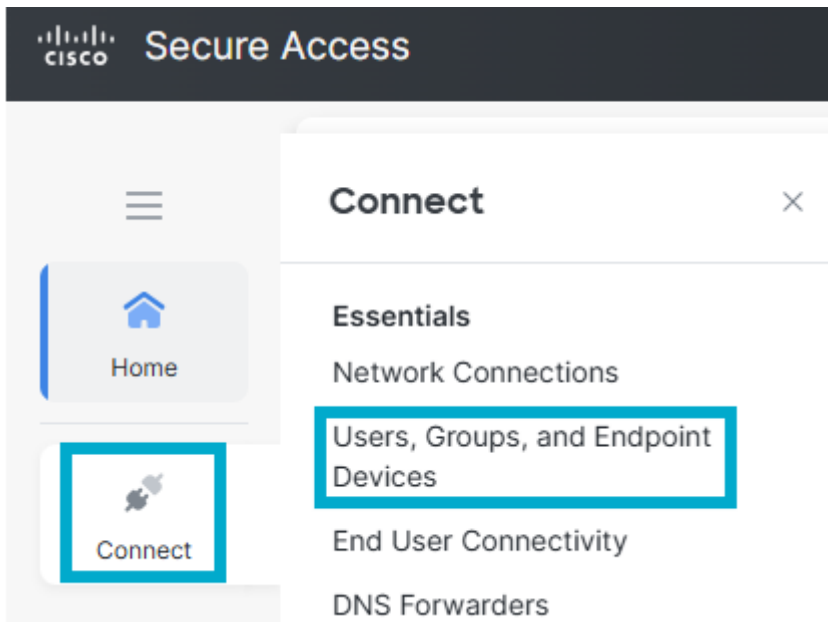


참고: 초기 프로비저닝 주기가 사용자/그룹을 프로비저닝하지 못하면 을 클릭합니다Restart provisioning. 이렇게 하면 Entra ID가 사용자 및 그룹의 첫 번째 동기화를 다시 시도합니다.

다음을 확인합니다.

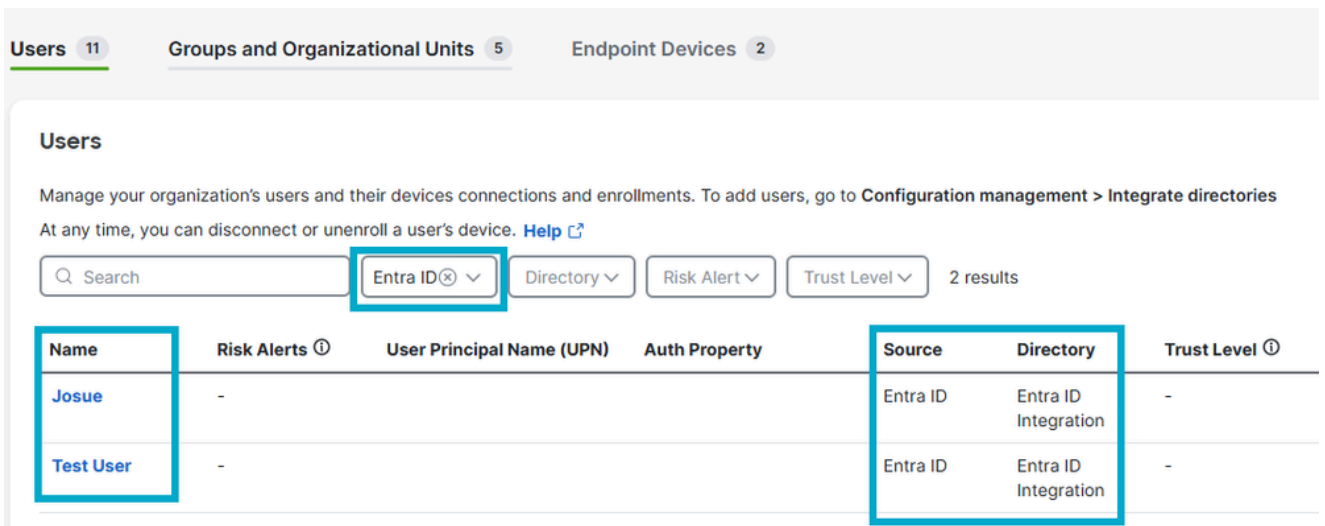
Cisco Secure Access의 Verity

- Connect(연결) > Users, Groups and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스)로 이동합니다.



Users and Groups in CSA

- Users를 클릭합니다.



CSA의 사용자 확인

- Groups and Organizational Units를 클릭합니다.

Users 11 **Groups and Organizational Units 5** Endpoint Devices 2

5 Groups 0 Organizational Units

Groups and Organizational Units

Manage your organization's groups and Organizational Units. To add new groups or OUs, go to **Configuration management > Integrate c**

Q Search Type ▾ Source ▾ Entra ID Integration ⊗ ▾ 2 results

Name	Type	Source	Directory
IT-Admins	Groups	Entra ID	Entra ID Integration
IT-Cloud-Admins	Groups	Entra ID	Entra ID Integration

Verify Groups in CSA

Entra ID에서 확인

- Enterprise Apps(엔터프라이즈 앱)로 이동하고 Cisco User Management for Secure Access(보안 액세스를 위한 Cisco 사용자 관리)를 클릭합니다.

Home Entra agents

Favorites ▾

Entra ID ^

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps ★

... > > > New provisioning configuration > Cisco User Management for Secure Access

Enterprise applications | All applications

MSFT

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications**
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

« + New application Refresh Download

Agent ID (Preview) has been moved to the Agent I

View, filter, and search applications in your organization

The list of applications that are maintained by your or

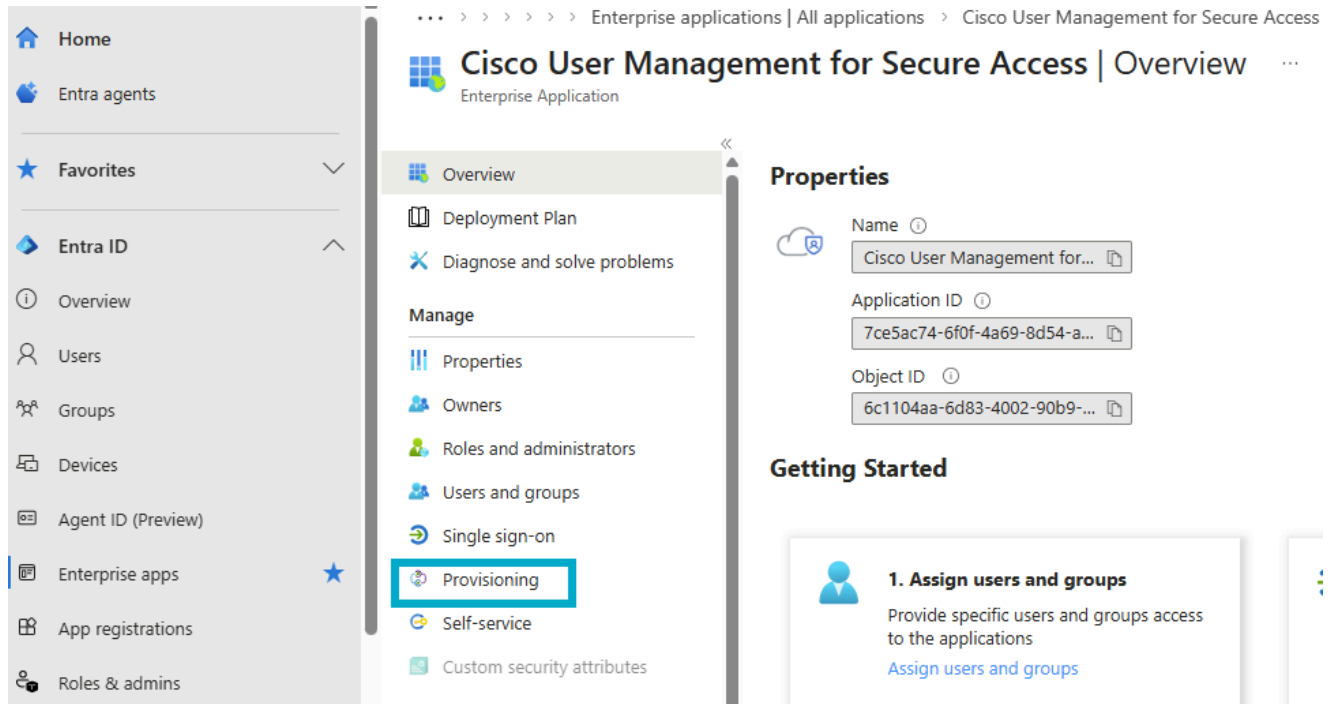
Q cisco user management

1 application found

Name

Cisco User Management for Secure Access

- Provisioning을 클릭합니다.



Verify in Entra ID

- Overview를 클릭합니다.

Cisco User Management for Secure Access | Overview

Overview

Provision on demand

Manage

Connectivity

Provisioning

Attribute mapping (Preview)

Users and groups

Expression builder

Monitor

Provisioning logs

Audit logs

Insights

Troubleshoot

New support request

Start provisioning | Pause provisioning | Restart provisioning | Delete configuration | Refresh

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user

Get started | **Overview** | Properties

Basic information

Name: Cisco User Management for Secure Access

Service principal object id

Job ID

Last cycle completed time: 3/18/2026, 10:27:27 AM

Current cycle status

Current cycle status: Incremental sync completed > Provisioning details

100% completed

GROUP	USER
2	2

Verify Provisioning in Entra

- Provisioning logs(로그 프로비저닝)를 클릭합니다.

App registrations > Enterprise applications | All applications > Cisco User Management for Secure Access | Overview > App registrations > Enterprise applicat

Cisco User Management for Secure Access | Provisioning logs

Overview

Provision on demand

Manage

Connectivity

Provisioning

Attribute mapping (Preview)

Users and groups

Expression builder

Monitor

Provisioning logs

Audit logs

Insights

Troubleshoot

New support request

Download | Refresh | Manage view | Got feedback?

Search Identity

Show dates as: Local | Date range: Last 24 hours | Action: All | Status: All

Date ↓	Identity	Action	Source system
3/18/26, 8:32:41 AM	Display name IT-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:41 AM	Display name IT-Cloud-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:39 AM	Disolav name IT-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:39 AM	Display name IT-Cloud-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Test User	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Josue	Create	Microsoft Entra ID

관련 정보

[ID 제공자 구성](#)

[Microsoft Entra ID에서 사용자 및 그룹 프로비전](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.